ChainGuard
A Firewall for Blockchain Applications using SDN with OpenFlow
September 27th, 2017

Mathis Steichen, Stefan Hommes, Radu State
mathis.steichen@uni.lu

SEDAN - Services and Data Management
SnT – Interdisciplinary Centre for Security, Reliability and Trust
Motivation

- Private blockchains have different vulnerabilities than public blockchains.
  - Data access requirements.
  - Targeting of nodes participating in the consensus mechanism.
- ChainGuard
  - Additional access control verification within the network.
  - Protects blockchain nodes from denial of service attacks.
Public blockchains

Transactions of Block n

Block n-1 → Block n → Block n+1
Public blockchains

- Everyone can propose new blocks and take part in the consensus mechanism.
- Large number of participating nodes:
Security in public vs. private blockchains

- Public blockchains
  - Large number of participating nodes.
  - Data is publicly available.
- Private blockchains
  - Small and limited number of nodes.
  - Nodes can have specific functionalities.
  - Can contain sensitive data.
Attack scenarios for private blockchains

- Brute forcing access control system to gain access to sensitive data.
  - Client data (banks)
  - Patient data (MyHealthMyData, eHealth)
  - General Data Protection Regulation

- Denial of service attacks to stop blockchain operations.
  - Target specific nodes.
    - Interrupt participation.
    - Disturb blockchain operation.

- Goals of ChainGuard
  - Prevent unauthorized nodes from participating and viewing the data.
  - Mitigate denial of service attacks targeting blockchain nodes.
ChainGuard

SDN-Controller

ChainGuard
Graylist
Whitelist
Blacklist

Guarded Blockchain nodes

Guarded Blockchain nodes

External Blockchain nodes

Malicious node

Internet
Software-defined networking

- Centralized control of the network.
- Dynamically implement access control within the network.
Permissioned blockchain - Multichain

- Bitcoin compatible, permissioned blockchain.
- Permissions are stored on the blockchain.
- Similar API
  - Get information about the blockchain.
  - Get information about peers.
    - Access control information.
Categorization of remote nodes

- Three groups
  - Whitelist: Nodes that are allowed to connect to the blockchain.
  - Blacklist: Nodes that are NOT allowed to connect to the blockchain.
  - Graylist: Nodes for which permission information is not yet available.
List implementation details

- List
  - Item 1
  - Item 2

- Actions
  - On arrival
  - On match
  - Timeout

- Item:
  - PacketIn info
  - Destination node info
  - Switch info
  - Arrival date and time
Transitions between lists

New connection attempt → New Item → Graylist

- Graylist: Action: Accept
  - Authorized connection (becomes peer)
    - Whitelist: Action: Accept
      - Peer leaves the network
    - Unauthorized Connection (timeout)
      - Blacklist: Action: Drop
        - No new connection attempt
Transition from the graylist to the blacklist

- New connection attempt
- Append new item to graylist
- Poll peer information
- Forward packets to destination
- Timeout expires and item transition to blacklist
- Block packets from source
Transition from the graylist to the whitelist

- New connection attempt
- Append new item to graylist
- Poll peer information
- Forward packets to destination
- Item transitions to the whitelist
- Node becomes peer
- Timeout would expire
Distributed denial of service attacks

• ChainGuard can mitigate denial of service attacks.
• ChainGuard can enforce access control on the network level.

• But:
  – Distributed denial of service attacks can lead to an overflow of the lists on the controller and of the tables on the switch.
• Solution:
  – Mechanisms that detect DDoS attacks.
DDoS - Capped graylist

- An attack is signaled by the overflow of the capacity limited graylist.

![Graylist diagram](image)
DDoS - Bucket token

- An attack is signaled by an empty bucket token.
Experiments

- Single attacker targeting the blockchain node.
- Multiple attack sources.
  - Capped graylist
  - Token bucket
DoS - Single attack source

PacketIn messages

Flow modification messages

Packets received at the target
DDoS - Capped graylist

![Graphs showing packet rate vs packets sent, packet rate vs PacketIn messages, packet rate vs flow modification messages, and packet rate vs packets received at the target.](image)
DDoS - Bucket token

PacketIn messages

Packets sent

Flow modification messages

Packets received at the target

Packet rate [1/s]
Conclusion

- ChainGuard: A Firewall for Blockchain Applications using SDN with OpenFlow
  - Provide access control and mitigate DoS attacks.
  - Two methods to mitigate DDoS attacks.
- Implementation details and experimental verification.
Thank you!